# REMARKS

Reconsideration of the above-identified application in view of the amendments above and the remarks following is respectfully requested.

Claims 1-47 are in this case.

Examiner has brought to Applicant's attention that claim 28 may not be statutory since the method may be performed mentally. Claim 28 as well as dependent claims 29-30 are hereby amended to to explicitly include all the steps being performed using a "computerized device". Claim 47 is hereby amended to further distinguish over the prior art in order to expedite the prosecution.

Examiner found that Applicant's reply filed on February 14, 2005 does not fully comply with 37 CFR 1.111(b) because the prior remarks did not explain how previously amended claims are patentable over prior art of record. Applicant hereby supplies the omission of the prior reply.

**The References and Differences of the Prior Invention Thereover:**

Prior to discussing the claims, Applicant will first discuss the references of the prior art of record and the novelty of the present invention and its unobviousness over the references.

The present invention involves a new type of "encryption"by achieving "randomness" produced by human action interacting with a "computerized device". Specifically, the present invention includes "randomly fragmenting" and "randomly shifting" data based on a human generated "random map".

Hulme ("Cryptography" 1899) discloses masking data in such a way that the data remains in order. In the present invention, the data does not remain in order.

An accurate term for Hulme's method is "masking" data because the letters of Hulme's message remain in order, only the message is masked and interspersed with letters not included in the message. "Shifting" data implies changing order in addition to "masking". Hulme does not disclose "random shifting of data according to a map".

British War Office ("Manual of Cryptography"). discloses alphabetic ciphers in which a previously determined parameter, *e.g.* two dimensional position or an integral number, is associated in one-to-one correspondence with each letter of the alphabet. British War Office does not disclose "random fragmenting" and "random shifting" of data. The "random fragmenting" and "random shifting" of the present invention does not generate such a one-to one correspondence.

Menezes et al. ("Handbook of Applied Cryptography")describe key transport based on symmetric encryption techniques. Menezes et al. (page 497) describe a prior art case of symmetric encryption using multiple symmetric keys. As an example of Menezes et al. , Alice is sending secret messages to Bob using a symmetric key. Eve is eavesdropping on the messages in order to obtain the key. Because Eve may succeed, the key must be changed frequently. Menezes et al. describe a conventional case in which a stack of symmetric keys is shared between Alice and Bob each key of the stack generated by an algorithm previously defined and shared by Alice and Bob. In principle, Eve on obtaining by eavesdropping a large number of the keys, may be able to determine the algorithm used to generate the keys. In the present invention, the keys are generated based on a "randomly map", not on an algorithm and therefore with the present invention it would be impossible for Eve to generate subsequent keys based on obtaining by eavesdropping a large number of sequential keys. (middle man attack)

Schneier (Applied Cryptography) in chapter 10, describes generating

symmetric keys with the use of a shared algorithm. In the present invention, the symmetric keys (or maps) that are shared are "fully" random since they are generated by "randomly fragmenting" and "randomly shifting" the data. Keys based on an algorithm cannot be fully random.

Sasich et al. (US patent 6,661,904) teach a method for using an image as a digital signature for remote transactions. Specifically, Sasich et al. teach a method to make a base image unique such as by embedding personal data in the base image. Sasich et al. do not disclose "random shifting" or "random fragmenting" of information according to a "random map".

Bocionek et al. (US patent 6,301,360) discloses a method to code information into an image, such as a chaotic image. The coding and decoding are performed by an algorithm. (see for instance Fig. 1a and Fig. 1b in which the coding and decoding are performed electronically. Hence, Bocionek et al. do not teach "random shifting" or "random fragmenting" of data.

Novaes (US patent 6,460,068) discloses a scheduler for testing applications. and does not disclose "random shifting" or "random fragmenting" of information according to a "random map".

Hoffberg et al. (US patent 5,774,357) disclose a human interface device and do not disclose "random shifting" or "random fragmenting" of information according to a "random map".

**Rejections under § 102(b)**

In the first office action, claims 1-2,7,9-13 were rejected under 35 U.S.C. §102 (b) as anticipated by Hulme ("Cryptography" 1899). and claims 1-2,6 were rejected under §102(b) as anticipated by British War Office ("Manual of Cryptography").

**Claims 28 and 47**

In order to expedite the prosecution, claim 1 in the prior amendment was rewritten as new claim 28. Claim 28 (currently amended) as well as parallel system claim 47 (currently amended) recite "randomly selecting", " randomly shifting" of "computerized data" , all the steps by a user using a "computerized device". Neither Hulme nor British War Office (nor any of the prior art references of record) teach "randomly shifting" of data according to a "random map" .

Claims 28 and 47 are currently amended to include "disordering" of the computerized data to further distinguish the present invention from Hulme and British War office. Hulme only masks the data, so that the data remains in order. British War Office also doesn't "disorder" the data rather replaces each unit of data with units of coded data in a one-to-one correspondence. Hence, also in British War office the data remains "in order".

**Rejections under § 103(a)**

Furthermore, there is no justification in any of the prior art references of record which suggests that these references should be combined, much less be combined in the manner proposed. It is well known that in order for any prior art references themselves to be validly combined for use in a prior art §103 rejection, *the references themselves* (or some other prior art) must suggest they are combined, as stated in *e.g.* re Sernaker 217 U.S.P.Q. 1,6 (C.A.F.C 1983):

> "Prior art references in combination do not make an invention obvious unless something in the prior art references would suggest the advantages to be derived from combining their teachings".

In line with this decision, the Board stated in Ex parte Levengood 28, U.S.P.Q.2d 1300 (P.T.O.B.A&I. 1993):

> "In order to establish a *prima facie* case of obviousness, it is necessary for the examiner to present *evidence,* preferably in the form of some teaching, suggestion, incentive or inference in the applied art, or in the form of generally available knowledge"

**Novel physical features of Independent claims 28 and 47**

**Produce New and Unexpected Results**

Applicants submit that the novel physical features of claims 28 and 47 are also unobvious and hence patentable under §103 since they produce new and unexpected results.

These new and unexpected results include a strong "encryption" method which avoids the excessive computational power and other well known complications of prior art public key infrastructure solutions. The keys are theoretically unbreakable being based on random strings generated by human actions. The present invention is lightweight and fast with negligible processing requirements. The present invention avoids "middle man" attacks.

As such, the present invention fulfills a long felt need as the public key infrastructure system (asymmetric keys) requires excessive amounts of computational power. As previously discussed, the present invention is superior to a symmetric key system since the present invention is based on random maps and not based on algorithms and therefore not susceptible to a "brute force attack" (page 30 line 1-2)

In view of the above amendments and remarks it is respectfully submitted that independent claims 28 and 47, and dependent claims therefrom are in condition for allowance. Prompt notice of allowance is respectfully and earnestly solicited.

Respectfully submitted,

Mark M. Friedman
Attorney for Applicant
Registration No. 33,883

Date: Apr 7, 2005